SECTION 4 TABLE OF CONTENTS

26 Aug 2004

Page

SECTION 4 TABLE OF CONTENTS, CONT.

Page

SECTION 4 TABLE OF CONTENTS, CONT.

Page

LIST OF FIGURES

Page

This page left blank intentionally.

4.0 PREPARATION AND ANALYSIS

This section provides an overview of DON and NMCI policies and requirements that must be considered in developing new releases or changing existing releases. Application of this information during the design and development of the release reduces delays in moving applications through the Testing, Certification, Accreditation, and Deployment processes.

4.1 DATA COLLECTION AND ASSESSMENT

A database catalog lists all applications that have been submitted for deployment in NMCI. This database is maintained by EDS and resides in the ISF Tools Database. The developer is responsible for conducting data analysis to eliminate duplication of effort and to ensure the upcoming release can operate in the NMCI environment. Appendix E lists the factors used to evaluate releases migrating into NMCI. The developer must obtain FAM approval prior to proceeding with development.

4.2 ENTERPRISE RATIONALIZATION

Enterprise Rationalization is the process of identifying which desktop and server-based applications, both COTS and GOTS, are required to support Command or DON missions, goals, and business processes. It includes the integration, consolidation, and elimination of applications and associated databases; improving standardization; enhancing security; and minimizing support costs. Rationalization policy and guidance is primarily the responsibility of the Deputy CIO (Navy), whereas service-level policy and guidance is the responsibility of the respective Service CIOs. Claimant/Marine Corps-level policy and guidance for rationalization of software applications is the responsibility of the CIO of the claimant/Marine Corps organization.

The DON-level enterprise rationalization process has a structured approach to information management framework; this includes functional and acquisition program managers to ensure horizontal integration (HI) of systems and databases. This process ties into the Enterprise Resource Planning and TFW initiatives. It includes identifying duplicative applications, older versions of applications, and applications that have completed certification, as well as working with the Navy claimants and Marine Corps organizations to resolve issues. FAMs lead this rationalization process.

4.3 DEPARTMENT OF THE NAVY APPLICATION DATABASE MANAGEMENT SYSTEM (DADMS)

To enhance the Navy success in effectively implementing NMCI, the CNO established a goal to reduce Navy Legacy Applications by 95% within one year (by May 2003). To accomplish this effort, the DON CIO directed the development of DADMS.

The DADMS was created as a tool to enable the FAMS to segregate applications by function, identify and catalogue application attributes, and manipulate information related to applications. It is intended to help reduce the number of applications needed to support the operation of the Navy IT enterprise.

DADMS supports the FAMs and FDMs in developing standard applications, databases, and data elements. It provides structure to maintain configuration control of all applications and databases across all DON networks. This helps the integration process to capture both the Navy and Marine

Corps existing IT business rules and requirements. Processes and procedures can be found on the Department of the Navy Chief Information Officer DON Application & Database Management System (DADMS) Home Page (https://www.dadms.navy.mil/) under "Policy and Guidance."

4.4 FAM PROCESS SUMMARY

FAMs and Command organizations employed short-term and mid-term rationalizations to decide whether to retain or eliminate applications. The short and mid-term rationalizations were iterative processes that employed a questionnaire to score, rate, and categorize applications. Developers and Commands populated the questionnaire. It was then scored automatically to help FAMs decide dispositions and prioritize applications. However, the questionnaire score was only a tool for the FAMs; the FAM made the final decision. In order to make the most reasonable decisions, the FAMs considered Command recommendations, requirements, and all available directives. The FAM high-level decision criteria can be generalized as follows for each application disposition:

- **Approved:** Applications identified as preferred, Gold Disk applications; applications that must be retained for a considerable timeframe; and the most current version, etc.

- **Allowed with Restriction (AWR):** Applications that had sufficient information provided in the questionnaires for FAM to maintain until further analysis could narrow the number of applications with redundant functionality.

- **Disapproved:** Applications that had unknown versions, no POCs listed, missing or incomplete questionnaire information, NMCI Application Ruleset failures, and duplicate records.

FAM Approved and AWR applications are slated for follow-on migration planning, analysis, and execution to identify and implement the "best" software solution for all stakeholders. The "best" solutions will be determined by implementing a business case analysis process, which considers the objectives and priorities of all stakeholders, including the objective to achieve the Navy goal for reducing applications supporting DON functional requirements.

For Navy-owned applications that need to be loaded onto a Marine seat, the appropriate Marine FAM should allow the application with restriction (AWR). For Marine-owned applications, the appropriate Navy FAM should do the same. The FAMs from both services should either approve joint mandated applications or designate AWR.

4.4.1 Failed Status for FAM Disapproved Applications

In the case of a FAM "Disapproved" application, the ISF Tools Database reflects the following information. Disapproved applications are marked as "Failed due to violation of NMCI Ruleset 13," which states that the candidate application is personal, nonmission, or nonbusiness related and is therefore prohibited in the NMCI environment. A failure letter is generated to document the assignment of this failed status.

4.5 NMCI APPLICATION RULESET

All applications are reviewed against the NMCI Application Ruleset for compliance. Applications found not to be in compliance with the ruleset are subject to FAM waiver, or are killed and removed from NMCI. Not all rulesets are waiverable. Appendix D provides a more detailed explanation of the ruleset requirements.

Developers are encouraged to consider development requirements specific to supporting IT-21, the Marine Corps Tactical Network (MCTN), BLII, and the TFW. The goal is to standardize applications and databases across all networks, if feasible.

4.6 FAM APPLICATION WAIVER PROCESS

For any required application that was discarded by the FAM in either short-term or mid-term rationalization, the “owning” Command may submit a waiver. In this scenario, the owner is the site and personnel that requires the application to support business processes and the mission. In most cases, the application requiring a waiver had been disapproved because of lack of information. The FAM process and the DADMS ***mandate*** that an application have a populated questionnaire with a unit identification code (UIC) signature, Command signature, and a developer signature in order for the recorded application to be retained in either an Approved or AWR status. Therefore, the owner must identify the application, search for it in DADMS, and have it waivered for Command and FAM approval.

Waiver processes and procedures can be found on the Department of the Navy Chief Information Officer DON Application & Database Management System (DADMS) Home Page (https://www.dadms.navy.mil/) under “Policy and Guidance.” **NOTE:** The FAM application waiver process should NOT be confused with the waiver submission to the NMCI DAA. A waiver for a port exception is only an interim technical solution process that does not generally involve any FAM interaction.

4.6.1 How to Waiver an Application

The owner must search for the application in DADMS, and it must not be a duplicate record. Once the record is found, the owner must click the waiver button to begin the waiver process. DADMS requires an additional questionnaire specific to the waiver. This questionnaire asks why the application waiver is being requested (i.e., due to an NMCI Application Ruleset failure, quarantine/kiosk status, expired waiver, etc.). All information must be populated in questionnaire steps 1 through 6, if applicable.

The DADMS main page provides assistance in filling out a questionnaire or questions on the FAM process under “DADMS Help.” Additionally, once a waiver is completed, the owner should notify the Command representative to ensure a review of the waiver and to obtain further guidance.

4.7 CERTIFICATION AND ACCREDITATION (C&A)

All DoD information systems that enter, process, store, or transmit unclassified, sensitive but unclassified (SBU), or classified National Security information, including contractor operated or owned facilities under DoD authority, must be certified as meeting minimum security requirements and be accredited for operation by a cognizant DAA. Owners and developers of legacy networks, systems, and applications wanting to transition into or connect to NMCI must document both system engineering activities and supporting security C&A activities to demonstrate to the Navy NMCI DAA that the network, system, or application meets the minimum IA requirements.

Existing Navy systems/applications often have not completed all DoD/DON-required security C&A processes defined in the DoD Inst 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Department of Navy IA Publications on C&A, the DON IA Pub 5239.13 (Volumes I and II). Many systems/applications were developed or acquired prior to the existence or implementation of the DITSCAP and current Navy IA requirements. Other systems/applications have been provided to the Navy and allowed to operate without supporting security or system configuration documentation. The lack of detailed development information, systems engineering, and security documentation regarding these systems makes it difficult for the Navy NMCI DAA to ensure that transition to NMCI can be accomplished within acceptable IA parameters.

If a system/application requires communications across NMCI boundaries, compliance with minimum IA requirements is essential regardless of CLIN or whether a system/application is hosted and managed by NMCI or the Government. Failure to identify the communications paths and to meet the minimum IA requirements will prevent the system/application from functioning properly.

To ensure that these requirements are fully documented and understood, NNWC, the NMCI DAA, follows the process defined in DoD Instruction 8510.1-M, DITSCAP Application Manual. This document provides detailed information on the DITSCAP process to assist the developer and Command in completing and submitting documentation for review and approval by the NMCI DAA.

Additional information pertaining to the DITSCAP process and document-generation tool is available at http://iase.disa.mil/ditscap/index.html

4.7.1 Purpose

The DITSCAP applies to C&A professionals, users, acquisition and maintenance organizations, developers, system integrators and procurement officials. Each community has a specific role in developing, procuring, employing, and operating an information system (IS) with an acceptable level of residual risk. These communities perform the following tasks:

- Identify the IA requirements, Level of Effort (LOE), and the C&A approval process necessary for successful deployment to NMCI,
- Define efforts required to ensure compliance with published DoD C&A policies while remaining DITSCAP compliant for existing fielded systems/applications.
- For a system or application in development:
  - Identify security requirements.
  - Design to meet those requirements.
  - Test the design against the same requirements.
  - Monitor the accredited system for changes or reaccreditations as necessary.

4.7.2 DITSCAP Application Manual Objectives

The objectives of the DITSCAP Application Manual are as follows:

- Assist and guide a developer or local system/application owner in constructing a DITSCAP of the current security posture of the system/application.

- Establish an evolving, yet binding, agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the DITSCAP becomes the baseline security configuration document.

- Establish a standard process, set of activities, general tasks, and a management structure to certify and accredit that the system or application is compliant with the IA and the security posture of NMCI.

- Support an infrastructure-centric approach, with a focus on the mission, environment, and architecture.

- Define processes that determine current technical details of IA, communications, and architecture associated with systems or applications in their “as-is” environment.

- Provide the guidance necessary to fully satisfy DoD/DON C&A requirements as defined by the NNWC NMCI DAA office.

4.7.3 Application and Scope

The DoD and DON C&A requirements apply to the following entities:

- Navy activities, organizations, contractors, and systems or applications, including all information systems that enter, process, store, or transmit unclassified, SBU, or classified National Security information, whether in Government-owned or contractor-operated-or-owned facilities under Navy authority

- Fielded Program of Record systems/applications that have not been accredited in operational environments

- Systems/applications that meet the requirements for operation within NMCI

- Systems/applications that select CLIN options to deploy into NMCI (CLIN 29)

- Systems/applications or networks that select CLIN options to connect to NMCI but retain some or all administrative and DAA control (CLIN 27 and CLIN 32).

4.7.4 NMCI DAA Policy for Certification and Accreditation of Applications on NMCI

In accordance with COMNAVNETWARCOM message 141945Z Nov 2003 / NIA 11-03, the NMCI DAA provides guidance for the post cutover application release deployment process. Table 3-1 specifies the type of C&A work required to obtain DAA approval. This table provides 12 scenarios to help determine the type of C&A work required to support the release.

The NMCI DAA has instituted the following policy that supports the NRDP for upgrades to existing releases and the introduction of new (emerging) releases in NMCI.

4.7.4.1 Simple Applications

For simple applications (client/desktop/standalone) being introduced for the first time or being upgraded to a new version, the NMCI DAA issues a three-year ATO upon successful completion of packaging, testing, and certification of security compliance by the Applications Lab. No further C&A work is required for these types of releases.

4.7.4.2 Complex Applications

For complex applications (client/server) where the server is resides outside NMCI and the desktop resides inside NMCI, upgrades to the client portion only require satisfactory completion of EDS packaging, testing, and certification. Upon completion of the certification, a one-year IATO is issued for the client portion, pending submission of required C&A documentation in accordance with DoD Inst 5200.40 and Navy IA Pub 5239.13 Series (as applicable).

4.8 INFORMATION ASSURANCE (IA)

IA is critical to the success of NMCI. Through enforcement of security procedures, NMCI enables users to access information and services with the appropriate security trust necessary to do their jobs. Defense-in-depth protection mechanisms are deployed in a layered fashion, forming boundaries at multiple levels within the security architecture of the desktop and network. These processes ensure resistance to attacks and minimize the possibility of a security breach due to a weakness (known or unknown) at any single security component. Defense-in-depth protection strategies provide security features to NMCI systems and data and include such features as confidentiality, integrity, availability, accountability, authentication, and nonrepudiation.

4.9 SECURITY

4.9.1 Boundary Protection

Figure 4-1 depicts a standard set of boundary protection, which has been incorporated into NMCI to protect interfaces within NMCI and other networks. The National Security Agency (NSA) Guide to Securing Microsoft Windows 2000 Networks, as published by the Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC), provides the framework for these protection standards. Boundary protections enforce the policies required to connect to external networks; provide security mechanisms for secure access to applications, and protect COIs residing within NMCI. Section 5.0 discusses this area in further detail.

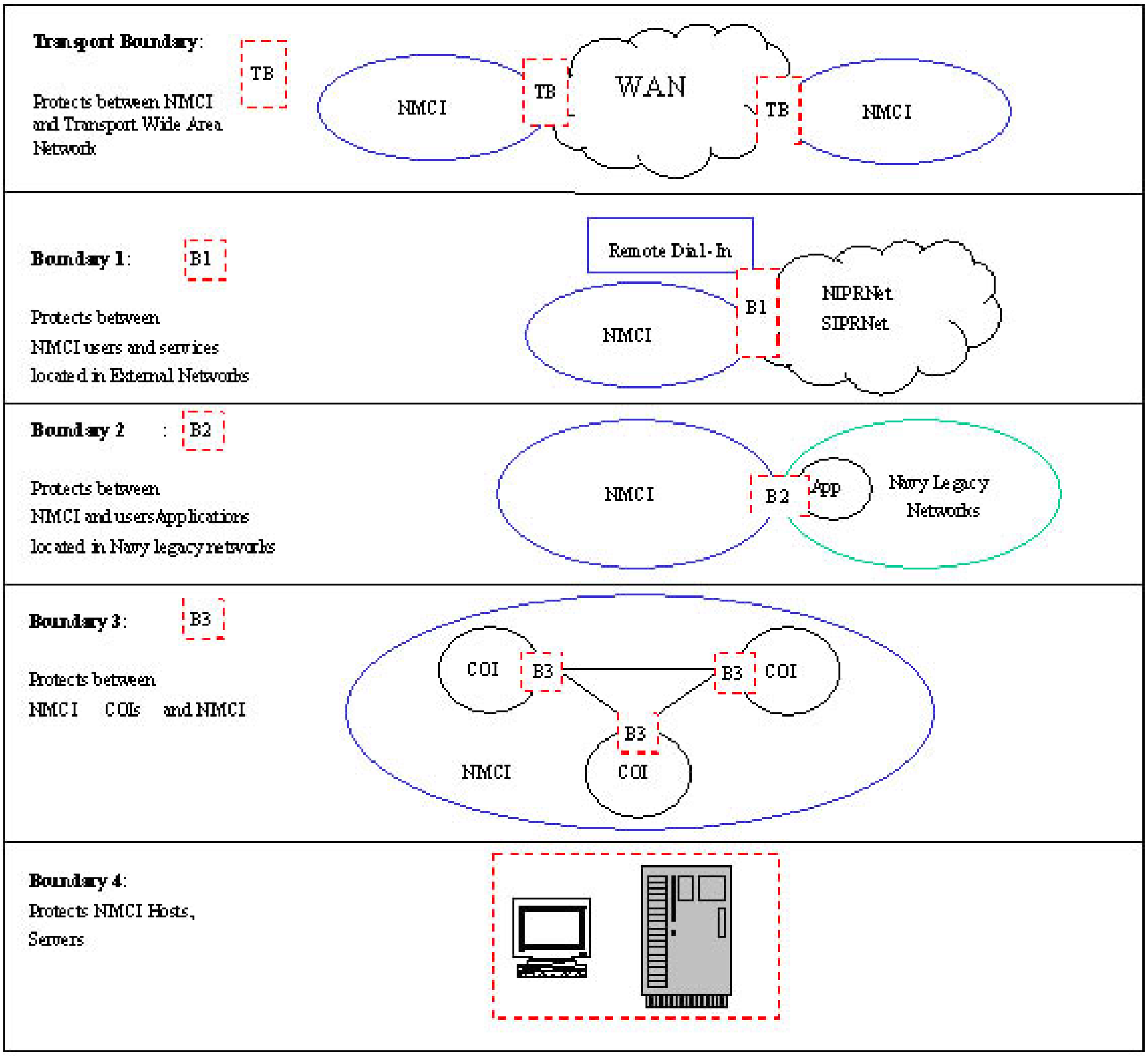
Transport Boundary:
TB
Protects between NMCI and Transport Wide Area Network
NMCI
TB
WAN
TB
NMCI
Boundary 1:
B1
Protects between NMCI users and services located in External Networks
Remote Dial-In
NMCI
B1
NIPRNet
SIPRNet
Boundary 2
: B2
Protects between NMCI and users Applications located in Navy legacy networks
NMCI
B2
App
Navy Legacy Networks
Boundary 3:
B3
Protects between NMCI COIs and NMCI
COI
B3
B3
COI
B3
NMCI
COI
Boundary 4:
Protects NMCI Hosts, Servers

Figure 4-1 Network Boundaries

4.9.2 NMCI Public Key Infrastructure & Directory System

NMCI employs Public Key Infrastructure (PKI) Class 3 certificates for strong user identification and authentication (I&A) and e-mail sign on. Infrastructure components are Public Key Enabled (PKE) for reciprocal authentication. NMCI implementation of DoD PKI provides accountability and nonrepudiation, and to a lesser degree, data confidentiality and integrity.

NMCI is compliant with DoD and DON security policies using two-way SSL and requires the installation of a DoD Class 3 PKI identity certificate on the workstation. Each user must contact the local certification authority to obtain a PKI certificate. Specific DoD implementation of PKI in the Navy can be found at the InfoSec website PKI primer: https://infosec.navy.mil.

4.9.3 Boundary 1 (B1) Conditionally Allowed Ports

Typically "conditions" are attached to the use of these ports that are “Conditionally Allowed” on NMCI. All applications that must communicate over the "Conditionally Allowed" ports must adhere to these "conditions." If proper compliance to the “conditions” is achieved, the application is permitted on NMCI (from an operational perspective). That is, the developer does not need to submit a "Request to Operate a Noncompliant System" to Space and Naval Warfare Systems Command (SPAWAR) Program Management Warfare (PMW)-161 for processing through CNO.

The developer or Command must provide sufficient information to the DAA that the application/release will comply with the “conditions” and ensure that EDS B1 firewall administrators understand the conditions. Each application that attempts to use the "Conditionally-Allowed" port must have the following information submitted in order to receive authorization to deploy the application:

- DITSCAP based package.
- Interim Authority to Operate (IATO) letter of recommendation issued by SPAWAR PMW-161 for large PORs.
- POR, or NNWC or local/developer DAA, for smaller systems (non-POR)
- Preexisting IATO submitted to NNWC for review with the C&A documentation.
- The total port, protocol, service, and direction of initiation (P/P/S/DI) requirement for system communications and topology. (Destination Internet Protocol (IP) addresses are required for specific port usage.)

For each legacy application/system transitioning to NMCI using the "Conditionally Allowed" ports, the NMCI DAA maintains a listing/registry to ensure that they have a complete picture of which ports are being used. This listing supports enterprise decisions for Information Assurance Vulnerability Alert (IAVAs), NAVCIRT Advisories, etc.

4.9.4 Active Directory (AD)

Within NMCI, security administration uses the basic features of the AD, groups, and organizational units (OUs). AD is a Microsoft trademarked directory service (DS) that provides the basic security policy enforcement and access control administration mechanism for NMCI. AD, which is an essential component of the Windows 2000 network architecture, presents organizations with a DS designed for distributed computing environments. AD allows organizations to centrally manage and share information on network resources and users while acting as the central authority for network security.

4.9.5 Security Objects: Group Policy Objects (GPOs)

The GPO enforces the operating system desktop security mechanism. NMCI uses the Windows GPO guidelines for some of its security enforcements. This guide does not include these guidelines; they are available to developers through NNWC and EDS. Paragraph 5.4 discusses this area in further detail.

4.9.6 Security Management

DON and EDS personnel jointly manage NMCI security, where the DON sets policy and EDS is responsible for implementation. Although the Security Operations Centers (SOCs) are staffed primarily with EDS personnel, the DON exercises Command Authority over EDS defensive Information Warfare activities. Security is managed in compliance with all relevant DoD and DON policies.

4.9.7 Firewall Policies

As a DoD entity, the Navy is bound by DoD directives, memorandums, instructions, manuals, publications, mandates, etc. that must be adhered to by its networks. In an effort to comply and protect its own information, the Office of the Chief of Naval Operations (OPNAV) has issued the Navy-Marine Corps Unclassified Trusted Network Protection Policy (UTN Protect) that can be found at the DoD PKI certificate enabled security website: https://infosec.navy.mil. Information, updates, and status of this policy can also be found at https://infosec.navy.mil/. (Authentication is required to access actual policy.) Developers of Navy Enterprise applications that must traverse through Navy network boundaries must familiarize themselves with this policy, ensuring that their applications pass through the boundaries and thereby increasing their chances to expedite testing and obtain application certification.

4.9.8 Desktop GPO Implementation

NMCI enforces Navy and Marine Corps security policies by facilitating Microsoft AD and GPO functionalities. EDS, through the use of Novadigm Radia manages installation, configuration, and updates to releases within NMCI. NMCI users are not permitted to install software, except on a Science and Technology (S&T) seat. As stated before, Novadigm Radia packages include settings in configuration files, set path variables, icon file location, application drivers, etc. If the release settings violate GPO policy, the developer must reconfigure the release to comply with policy requirements.

4.9.9 File and Registry Permission

NMCI client images contain file and registry entries that provide appropriate permissions designed to conform to security requirements while allowing most releases to function properly. The following paragraphs describe how these settings affect applications deployed to NMCI clients.

4.9.9.1 File Permissions

The NMCI user desktop is a single partitioned C: drive; and the client image has special permissions. The GPO only allows users and applications to create folders and files in designated areas of the file structure. The following restrictions apply:

- NMCI seats are set with the NMCI EDS screen saver. The screen saver cannot be changed.

- Users can create subdirectories in the root directory.

- Applications can create subdirectories in the C:\PROGRAM FILES directory during installation.

- All operating system level files (autoexec.bat, System32, etc.) are not available for update by applications. The C:\WINNT directory can be written to or appended, but not overwritten.

- Desktop users may not change application files. Application files are distributed to the user's desktop using the AD, Novadigm Radia, and Gold Disk processes.

- Releases deployed to NMCI clients must be placed in subdirectories below C:\PROGRAM FILES. NMCI requires that release data be stored in the user's "My Documents" subdirectory. The location of the "My Documents" subdirectory should be obtained programmatically because this is not the same for all users / profiles. For example, terminal services users have their My Documents subdirectories redirected to their home subdirectories on the network.

To ensure that NMCI workstations are both secure and stable, users (and applications) are allowed to write only in designated folders on their local hard drive. These permissions are enforced using the Windows 2000 GPO.

4.9.9.2 Registry Permissions

Registry permissions change periodically. For current registry permissions, refer to the GPO information provided by NNWC and EDS. As with file permissions, Radia can write to all areas of the registry during installation of the application through the system account. However, once the application is installed, the user is restricted to the areas governed by the GPO while running the application. Therefore, the application should be designed to only write to those areas during runtime.

4.10 INFORMATION ACCESS & SYSTEM SERVICES

4.10.1 CLIN

The NMCI ISF provides services to a range of Navy and Marine Corps end points or service delivery points (SDPs). These SDPs include voice, video, and connection points for end users, general NMCI enterprise, and interfaces to other DON and DoD communications environments. Specific services to be provided to the end points vary but include the IT services listed by CLIN.

4.10.2 File and Print Services

File and print services are two of the most fundamental services within NMCI. File servers provide secure storage space for both public and private files. Print services allow users to produce black and white, color, or transparent hard copies of work created with NMCI hardware and software. Both services rely on the server platform and are connected to the user through the physical network.

4.10.2.1 User Identification and Access

For safety, server physical access should be limited to individuals who are experienced network administrators. Authentication Windows 2000 user access technologies authenticate these individuals. If an individual cannot be authenticated, server access is not granted to that server or any services operating on that server.

4.10.2.2 Computer Virus Protection

NMCI proactively provides virus monitoring at multiple levels within the NMCI infrastructure. Since virus definition, operating system patches, and other updates may occur automatically, the desktop computer should remain on overnight, with the user logged off, to allow network-managed software housekeeping.

4.10.3 Print Services

AD manages the Microsoft Windows 2000 print subsystem and allows a user to query the AD for available printers, as well as the default printer. Application developers should use AD to determine that a printer has the required print capabilities.

4.10.4 File Storage Services

User accounts are allocated 1 gigabyte of storage on a file server. Additional public storage can be purchased in 10-gigabyte increments by requesting a Task Order (TO) under CLIN 0016. Storage space is divided as follows:

- **Private**: 700 MB
- **Public:** 100 MB (pooled and controlled at Command level)
- **Growth:** 200 MB (25%)

For account services, each seat (red, white, blue, or deployable) comes with two unclassified accounts. Unclassified user accounts can be aggregated and used to provide unclassified access through existing unclassified NMCI seats.

Table 4-1 lists the available following drive letters and backup routines.

Table 4-1 Available Drive Letters and Backup Routines

Drive	Description	Incremental	Full Backup	Shared
C:	My Documents - local desktop. GPO rules are applied	None	None	No
H:	(Home) network directory for a user's private files or storage	Nightly	Weekly	No
S:	(Shared) network directory. Command public files or storage	Nightly	Weekly	Yes

4.10.5 File Sharing

EDS implements login scripts to map file shares. Each user has an "H:" and an "S:" drive mapped on a specific machine through a login script. The "H:" drive is the private drive of the user and cannot be shared. The only file sharing exists on the "S:" drive, and that file sharing is limited to the public portions assigned to that specific user. Standard Microsoft file sharing rules and permissions apply. The "C:" or local drive and all of its contents are not shareable. This policy is standard throughout the

NMCI environment. Additional shares should be mapped with a drive letter that is consistent across the NMCI enterprise.

Users do not have delete or change permissions and cannot take ownership of files they did not create; nor are they allowed to share private storage or create shares on their desktops. Users should verify that adequate space is available on a network drive before writing files to these resources. Developers must not to remap the public (S) and private (H) network directories.

4.10.6 Personal Storage

Users are assigned a network drive that points to their private data (H:\), and cannot provide shared access. To share files with others, users must use the Command shared network drive space (S:\).

The home drive (H:\) points to a user's personal file space located under the USERS directory on each file server. This space stores files used only by the individual user [e.g., files such as the mail personal storage (.pst) file].

4.10.7 Shared Storage

Within NMCI, shared storage is allocated by Command. Folders and files located in this shared storage permit users to read, write, and execute files. Users may create and delete folders. Designated individuals within the Command may control access to the shared storage. NMCI shared storage is not accessible from outside the NMCI enclave.

The shared drive (S:\) points to group data. Each Command is given a folder containing the shared space for all of its users. The directory is shared at the Command level, and the Command designates which user accounts are made owners of the directory. By allowing the designated owner to control access using New Technology File System [Microsoft](NTFS) permissions, the Command can exercise the greatest level of flexibility over the allocation of this storage space.

4.10.8 File Share Naming Conventions

File sharing follows standard Universal Naming Convention (UNC) paths. Refer to Table 4-2. AD uses the following format for file share naming:

\\CCCCCC\LLLL\SSSSSSSSS

Table 4-2 File Share Naming Conventions

Symbol	Represents	Character Count
CCCCCC	Command	Variable
LLLL (Optional) (Local Shares Only)	Site Identifier	Four
SSSSSSSSS	Share Name	Variable

File Share Naming Examples:

\\SPAWAR\SPOT\Group161
\\MARFORPAC\PLMS\SOFTWARE
\\NAVAIR\PAXR\ADMIRALS SHARE

4.10.9 Printer Naming Format

Printer names may be up to 80 characters long. The standard NMCI printer driver is Postscript. Refer to Table 4-3. AD uses the following format for network printers:

\\LLLL\BBBBBB\FF\RRRR\OOOOOO

Table 4-3 Printer Naming Format

Symbol	Represents	Character Count
LLLL	Site Identifier	Four
BBBBBB	Building Identifier	Variable
FF	Floor Identifier	Variable
RRRR	Room Identifier	Variable
OOOOOO (Optional)	Printer Identifier	Variable

Printer Naming Examples:

\\PAXR\Bld6\02\28\HPLJ5
\\FALL\B421\01\02\HPLJ5
\\MRMR\BLD5\01\331\HPDJ740

4.10.10 Messaging and Collaboration

NMCI messaging uses the Microsoft Exchange 2000 suite. The following paragraphs explain the system services of this suite.

4.10.10.1 E-Mail Addressing

User Principal Name (UPN)

E-mail addressing within NMCI use the UPN format that follows industry-accepted Simple Mail Transport Protocol (SMTP). A UPN is a multivalued attribute of each user object that the system administrator can set. UPN allows the underlying domain structure and complexity to be hidden from users. For consistency, the UPN and SMTP address format are identical.

The UPN is unique across NMCI. The naming convention has been adopted as follows:

- Firstname.lastname@service.mil (where service represents Navy or Marine Corps)

In the case of multiple users with identical names, the following additional conventions are used to establish uniqueness in the order of precedence:

- Firstname.m.lastname@service.mil where m represents middle initial
- Firstname.m.lastname#@service.mil where # represents a unique numeric identifier starting at 1.

Examples of UPNs for several Joe Users are:

joe.user@navy.mil
joseph.user@usmc.mil
joe.k.user@navy.mil
joe.k.user1@usmc.mil
joe.k.user2@usmc.mil

4.10.10.2 Mail-Enabled Public Folders

To allow multiple users access to a common mailbox, mail-enabled public folders have been implemented. These folders appear in the global address list as a mail recipient for Microsoft (MS) Outlook clients. Users that require this access are granted the appropriate e-mail permissions (view, send as, etc.). See the Microsoft Developer Network (MSDN): http://msdn.microsoft.com/.

CAUTION: Not all features are available within the NMCI security model. Developers must understand the restrictions implied by group policy and lockdown in order to determine which features are available.

4.11 PLATFORMS

4.11.1 Client Seat

NMCI client seats are EDS-managed seats. Therefore, users do not have administrative rights to desktop configuration or software installation. The basic client seat is delivered loaded with the latest standard Gold Disk configuration. Additional components can be installed on a client; however, an administrative facility pushes these to the seat. End users cannot add software to their seat;

IMPORTANT: Content developers should verify that client plug-ins and components are available and compatible.

4.11.1.1 NMCI Standard Desktop Configuration CLIN 0001-0004

The CLIN Service Matrix provides numerous options for standard desktop configurations. This matrix contains detailed information on the seat services and the Service Level Agreements (SLAs) included with various seats. Additional information on the desktop CLINS is available at http://www.nmci-eds.com/clinlist.htm.

IMPORTANT: Developers should consider peripherals when developing an application. They should consult the Microsoft Compatibility List.: http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/

As long as the peripheral has a Windows 2000-compatible driver (either from Microsoft or from its own manufacturer) and it does not violate any IA rules or SLAs, it should be able to transition into NMCI.

Legacy desktop single-user devices should transition with no additional fees as long as they are "plug & play". Legacy network multiuser devices need a CLIN 29 request.

The following NMCI standard desktops are available:

- Fixed Work Stations: Red, White, Blue, and Thin Client
- Portable and Ultralightweight Portable Seats
- Embarkable Work Station: Full Service and Limited Service
- Embarkable Portable Seat: Full Service and Limited Service

4.11.2 Science and Technology (S&T) Seat

This seat upgrade accommodates the special requirements of the S&T community by allowing the end user to reconfigure hardware and software without EDS intervention. This seat employs architectures and policies that are in accordance with the NMCI EDS security requirements. Customer support is limited to those services offered by EDS and not extended to software or hardware loaded and configured by the user. EDS is not responsible for SLA performance directly impacted by these seats due to the associated relaxed CM policies. The S&T desktop provides the latitude for those who need a software development platform and the ability to access settings and file locations that are restricted on normal NMCI seats. To order an S&T seat refer to CLIN 0038AA-AH.

The S&T seats provide the following characteristics:

- Allow rapid hardware reconfiguration
- Allow collaborative work and data-file sharing
- Allow software to be personally loaded to the desktop
- Connect to non-Windows 2000 operating systems (Solaris V8)
- Support nonstandard protocols
- Meet high bandwidth requirements
- Provide appropriate security mechanisms

S&T seats reside behind the Boundary 3 (B3) firewall, which protects the NMCI. Further information about S&T seats can be found at http://www.nmci-eds.com/userinfo_sandtguide.htm. A detailed description of the CLIN list can be found on EDS web site at http://www.nmci-eds.com/clinlist.htm.

Developmental seats require elevated user privileges, including installing, removing, and compiling code. Because of this elevated privilege and increased risk potential, the developer community was placed in a COI to separate it from the normal user community. This protects the bulk of NMCI users from the elevated risk, while permitting the developer community to perform application development.

The NMCI DAA has delegated the responsibility of deciding what software or hardware is loaded to seats within the developer community to the local DAA. This could be the commanding officer (CO), officer in charge (OIC), decision height (DH), or PM lead of the unit/division/workshop/program. The

S&T user communities are given "keys to the kingdom" (access to the basic seat configuration) so they can manipulate their S&T seats as required. The Navy NMCI DAA expects local DAAs to be responsible for conducting themselves within their professional roles, to include installing or deleting applications within their development communities. EDS is not going to install applications on S&T seats other than initial loadout, which is the Gold Disk plus CLIN options, and perhaps part of a rationalized list. The user is responsible for any changes to the S&T seat after the initial loadout. If the installed development software impedes the ability of the user to access NMCI services (mail, print, file shares, etc.), the user is responsible for rebuilding or reloading to initial specifications and starting over. Alternately, a user could call the NMCI Help Desk and risk a MAC charge if the problem was not an EDS issue with basic services.

4.11.2.1 S&T Seat Precertification

As an interim measure until the Precertification CLINs are available, an S&T seat can be configured and used to support release Precertification testing. S&T seats have a relaxed GPO that allows the user administrator rights to load the necessary software required to perform this function. At a minimum, the S&T seat must be configured with the latest version of the NMCI Gold Disk load set, the current version of the NMCI seat GPO, Windows 2000, and appropriate software that monitors and collects data on the ports, protocols, and services used by the release.

The developer must follow all prescribed Precertification requirements contained in Paragraph 6.5.4. The following steps are performed as part of this process:

1. Ensure the S&T seat is properly configured to support Precertification testing.

2. Install a clean version of the release media on the seat. This also includes any dependent or supplemental media required for the release to operate properly.

3. Run the application and verify that it operates when supported by the Windows 2000 operating system and that it does not break or otherwise alter the operational capability of the Gold Disk load set.

4. Verify the desktop security and ensure the release interfaces with and is compliant with the NMCI GPO standard.

5. Capture the ports, protocols, and services used by the release for network connectivity. The developer should know both the outbound and inbound ports and protocols used by the release.

6. Document results of the Precertification test and include them in the RDP.

4.11.2.2 NMCI S&T Desktop Configuration CLIN 0038

This seat upgrade accommodates the special requirements of the S&T community by allowing the end user to reconfigure hardware and software to without EDS intervention. This seat employs architectures and policies that are in accordance with the NMCI ISF security requirements. Customer support is limited to those services offered by EDS and not extended to software or hardware loaded and configured by the user. EDS is not responsible for SLA performance directly impacted by these seats due to the associated relaxed CM policies. More detailed information on S&T seats configuration and available options is available at http://www.nmci-eds.com/clinlist.htm

4.11.2.3 Personal Digital Assistant (PDA) Applications

PDAs are approved for use within NMCI, as governed by policies in a series of NMCI Information Advisories (NIAs), NMCI Information Bulletins (NIBs), and Naval messages. The CLIN 0023 catalog lists the acceptable PDAs. Refer to http://www.nmci-eds.com/clin023.htm.

The NMCI DAA intends to issue a type accreditation for applications that reside within the Palm operating system. Other operating systems will be addressed later. These include applications that are preloaded "out of the box" and include the *Documents to Go* software (MS Word, MS Excel, and PowerPoint). The NMCI DAA handles add-on and custom applications that reside on an NMCI PDA on a case-by-case basis.

The packaging, testing, certification, accreditation, and deployment of these applications follow the existing NRDP, as explained in Section 6.0. Refer to COMNAVNETWARCOM message R 051645Z DEC 03.

Sites/Commands requiring a PDA application should use the RRPTE process contained in Section 3.0 to determine if the required application is already available in the ISF Tools Database Application Catalog or through CLIN 0023. If a required application cannot be obtained through the RRPTE process, the site/Command needs to introduce the release as a new (emerging) release through the NRMP.

4.11.2.4 Legacy Peripherals

USB devices that do not require software drivers are allowed for use within NMCI, with the exceptions of the Naval Nuclear Propulsion Information (NNPI) and USMC COIs.

Legacy peripherals are connected through CLINs 0027 and 006 (if needed). They do not require additional work if the driver is on the MS 2000 driver library. Complex peripherals have configuration issues and must use CLIN 0029 for driver deployment. Most will be accomplished using a Physical MAC.

4.12 NMCI APPLICATION SERVICES

This paragraph describes services available to developers as part of NMCI. Additional development services may be added over time. This guide will be updated as services are added.

4.12.1 Service Request Management (SRM)

The primary objective of SRM is to provide a uniform environment where all NMCI orders are processed timely and records of all changes are maintained. SRM accomplishes this by the following:

- Provides timely and accurate data
- Strictly enforces Enterprise data standards and business rules
- Streamlines dataflow

- Standardizes data access
- Facilitates access to commonly used Enterprise data
- Improves quality, completeness, and consistency of data values
- Improves data access speed
- Eliminates costly, time-consuming, and error-prone manual data handling
- Facilitates reporting

Developers use the service request for the Certification CLIN to support the certification of their release. Additionally, developers use a service request (MAC or Distribution CLIN) to support the deployment of their release. Application developers ***must*** work with their CTR/ACTR for service request submittal. (A CTR/ACTR is a designated person on the MAC Authorized Submitter List.) A description of the service request process follows.

4.12.1.1 Certification CLIN

Before EDS begins processing a release through Testing and Certification, the application developers' CTR/ACTR must complete a service request for Certification and submit it to the SRM Team. The SRM Team validates the request to ensure that the release is FAM approved, the request is filled out properly, and a CDA RFS is entered into the ISF Tools Database.

Once the service request has been validated, the SRM Team creates a Remedy Ticket. The Remedy Ticket is routed to the Applications Team to prepare for testing once the Applications Lab receives the Application Submission Packet. Refer to Paragraph 6.6.2.

4.12.1.2 Deployment Service Request [Moves, Adds, Changes (MAC)] or Distribution CLIN

For NRDP deployment, the application developer is required to use either of two methods:

- For individual or small numbers of NMCI seats, use a MAC.
- For large numbers of NMCI seats, use a Distribution CLIN.

The application developers' CTR/ACTR must submit this service request to EDS 30 days prior to completion of Testing and Certification. Failure to submit the deployment service request by the deadline will delay application deployment to the seats.

Normally, the release is packaged (Radia) for electronic deployment into NMCI and is supported by either an administrative (Admin) MAC or a Distribution CLIN. If the release cannot be packaged for electronic deployment, the only method available is to use a Physical MAC.

NOTE: Local load uses a physical MAC at the local site/Command only.

Once the service request has been validated, the SRM Team creates a Remedy Ticket. The Remedy Ticket is routed to the Applications Team to prepare for deployment after the application has been certified and ECCB approved.

For information about site/Command-requested deployment of a release, refer to the RRPTE process, Paragraph 3.6. More detailed information on admin MAC options is available at http://www.nmci-eds.com/clinlist.htm

4.12.2 Gold Disk

The NMCI Gold Disk contains standard desktop products and services to be installed on every NMCI client machine. Contents of the Gold Disk are updated as NMCI evolves and are managed through the NMCI Change Control Process. A review of the latest Gold Disk contents is available at http://www.nmci-eds.com/downloads/Gold_disk_contents.pdf

4.12.3 NMCI Server Connectivity CLIN 0027

Application server connectivity is a service that provides NMCI connectivity to legacy application servers for Navy and Marine Corps organizational, operational, and functional applications to meet mission requirements. This service meets peak network loading requirements of users for replication, but does not include server and database maintenance and administration. More detailed information on the various server connectivity options is available at http://www.nmci-eds.com/clinlist.htm.

4.12.4 NMCI Legacy Systems Support CLIN 0029

Legacy Systems Support provides initial integration services for emerging operational and functional systems to enable them to run on NMCI. Legacy System Support can also provide additional services beyond basic integration. These additional services provide a range of options that include, but are not limited to, NMCI EDS hosting of applications, operations, and maintenance support; database management; and training, if ordered. This service may include participation of the NMCI EDS in business process reengineering activities. These items are separately priced in individual orders and can be applied to legacy systems that have been integrated to run on NMCI as part of basic service during initial NMCI implementation. Future options will be available under this CLIN to support certification and Precertification of releases in support of existing applications, and for new (emerging) releases being introduced into NMCI for the first time. More detailed information on Legacy Systems Support is available at http://www.nmci-eds.com/clin029.htm.

4.13 COMPONENTS

Components are reusable programs that can be used as building blocks with other components to provide common services when building an application. Only standard Windows 2000 Professional components are provided in the NMCI Gold Disk.

4.14 DIRECTORY AND REGISTRY PERMISSIONS

Releases must be written in accordance with MS Windows 2000 standards to ensure compliance with Navy certification standards. In some cases, the DON establishes specific permission standards that must also be included in the release.

Information on Microsoft directory and registry permissions is available at http://www.microsoft.com/windows2000/. For information on Navy/Marine Corps specific permissions, contact the NMCI Help Desk.

4.15 BROWSERS

4.15.1 Microsoft Internet Explorer Version 5.0 or Greater

4.15.1.1 Plug-ins Provided on Gold Disk

The current set of plug-ins provided by the Gold Disk is available at http://www.nmci-eds.com/downloads/Gold_disk_contents.pdf.

EDS is evaluating additional plug-ins for inclusion in the NMCI Gold Disk. Appropriate plug-ins will be included in future releases of the Gold Disk. The Novadigm Radia server may also push plug-ins to desktops.

4.15.2 Netscape Communicator 4.76

Netscape is included on the NMCI Gold Disk. It is provided as a service for compatibility with existing systems and is not supported by NMCI. All new (emerging) releases should be developed to support the NMCI default browser, Internet Explorer (version 5.0 or later) unless constrained by international treaty or other business requirement to use Netscape.

4.15.3 Browser Security

NMCI implements the DoD Mobile Code policy. The DoD Mobile Code Policy defines the categories of mobile code and provides criteria for use within the DoD.

The policy is available at http://iase.disa.mil/policy.html

4.16 EMULATION

4.16.1 Terminal Services

From a developer’s perspective, the Microsoft guidelines are the recommended standard for how to design and construct applications to run in a “multiuser environment,” such as an environment with terminal servers.

Microsoft guidelines for Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition are available at http://www.microsoft.com/technet/

4.16.2 Product Supported

Reflection is the de facto standard terminal emulator that is included on the Gold Disk and is a standard application included on every NMCI seat. Reflection supports IBM, Hewlett Packard (HP), UNIX, Open Virtual Memory System (VMS), and X Suite environments.

4.17 ISF TOOLS DATABASE

When ready to start the approval process for a desktop application, the developer must enter the application into the ISF Tools Database, which is the current authoritative source for NMCI applications. Only developers may enter new (emerging) releases.

The ISF Tools Database is available at http://www.nmci-eds.com/transition.htm (transition link) or https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp (direct link).

Application developers/owners must obtain an ISF Tools Database developer account and submit a CDA RFS to ensure that their releases are listed and available for certification for NMCI according to Navy enterprise standards and EDS. The goal is to ensure that applications are necessary (rationalized), appropriate, and can function within the NMCI environment. Once ISF Tools Database access has been granted, developers can access the database to perform their duties. These duties include checking certification testing, viewing application survey data, adding additional applications, submitting applications, and viewing reports, based on the level of access granted by the Command POC.

In preparation for receiving an application push from either a newly certified update or a new application distribution, the Command CTR is responsible for updating the affected rationalized list in the ISF Tools database/RFS. If the ISF Tools database is not maintained, NET cannot be updated properly. If the ISF Tools database, and thus the NET database, is not updated properly, future Application Mapping to a new or upgraded release will not function properly.

> **NOTE:** Application Mapping in NET can only occur if the application currently resides on the rationalized list in the ISF Tools Database for the ordering Command.

If the release replaces an existing application on the site/Command rationalized list, the old application is removed just prior to deployment of new release. This step ensures that the application inventory for the site/Command reflects an accurate inventory of all applications deployed within the site/Command.

For more information, application developers should download and review the ISF Tools Database User Manual on the Splash page of the ISF Tools Database or contact the ISF Tools Database POCs. See EDS POCs in Appendix C for further assistance.

4.18 NMCI HELP DESK SUPPORT

NMCI customers can call, e-mail, or fax messages to the NMCI Help Desk and receive assistance 24 hours a day. Personnel using e-mail are encouraged to direct inquiries to the Help Desk center closest to them: Norfolk, VA, or San Diego, CA.

Phone	1.866.THE-NMCI
Fax	1.877.FAX.NMCI
Norfolk E-mail	HelpDesk_NRFK@nmci-isf.com
San Diego E-mail	HelpDesk_SDNI@nmci-isf.com

4.18.1 Level 1 NMCI Help Desk Support

The NMCI contractor is responsible for Level 1 NMCI Help Desk Support.

4.18.1.1 Global Outreach

NMCI Help Desk agents are located in state-of-the-art network operations centers in Norfolk, VA, and San Diego, CA. Supported by advanced call center automation technology, the agents are equipped to field NMCI user inquiries from across the globe.

4.18.1.2 Personalized Service

NMCI Help Desk services are available to support classified and unclassified data seat holders 24 hours a day, seven days a week, and 365 days a year.

NMCI Help Desk agents are qualified and ready to resolve any of the customer issues outlined below. Other members of EDS are also available to answer general questions about the NMCI program, address site-specific issues, or escalate persistent problems for resolution.

Technical & Application Support

- Problem resolution
  - Laptop (including network connectivity)
  - Workstation (including network connectivity)
  - Software
  - Printer
- Application support
- Password resets

Business Support

- MAC requests
  - Process and execute approved user requests
- User account services
  - Create
  - Modify
- Data seat hardware requests
  - Deinstall
  - Move and reinstall
  - Change
- CLIN requests
  - Acquire
  - Install
- Seat upgrade requests

4.18.1.3 Level 1 NMCI Help Desk Support to the Release

The contractor-provided NMCI Help Desk support is restricted to determining whether the client or network is the cause and then remediating the problem, if possible.

If neither client nor network is determined to be at fault, the NMCI Help Desk agent performs further application troubleshooting, as dictated by developer-provided procedures. If the problem persists, the customer's trouble ticket is escalated to Level 2 support.

4.18.1.4 Developer Support to the NMCI Help Desk (Level 1)

The developer or application owner should provide the Level 1 NMCI Help Desk with initial troubleshooting questions to perform immediate issue-resolution remediation on the application.

4.18.2 Level 2 and Higher NMCI Help Desk Support

The developer or application owner is responsible for Level 2 and higher NMCI Help Desk support. Level 2 NMCI Help Desk support should be coordinated with the NMCI contractor providing Level 1 support. For example, Level 2 NMCI Help Desk POCs should be available to the Level 1 agent for immediate customer referral.

4.18.2.1 NMCI Help Desk Manuals

NMCI Help Desk Manuals include the following documentation:

- System Administrator's Manual
- User Manual
- Software Version Description
- Preparation and Analysis
- System Administrator's Manual

User Manual

The User Manual is intended to provide the end user with the information needed to operate the software application. An updated version of this document may not be required for every release of the software application if the contents of the release are only fixes to known issues.

The User Manual has the following sections:

- **Software Inventory:** Lists all components that comprise the software application.

- **Environment and System Configuration:** Provides details.

- **System Overview:** Provides the operator with the main concepts of the software application. This section should briefly describe the Concept of Operations if a separate document has not been developed.

- **Referenced Documents:** Includes any standards (Government and Industry), operational documents, technical documents, and any other documents that are related to the software application.

- **Security Requirements:** Clearly identifies requirements for all aspects of the software application.

The operating instructions for the software application provide keystroke instructions to the user. The instructions cover all software modules and are organized according to common usage or accomplishing specific tasks in the software.

Software Version Description

The Software Version Description document provides information specific to the version of the software being released. The information provided focuses on the changes to this version of the software application from the previous. Information in this document includes Software Inventory, overview of the functionality of the released software, Installation Instructions, Referenced Documents, Environment and System Configuration, Security, and known issues. This document is required for every release of the software application.

Installation Procedures

The Installation Procedures is intended to provide the installer with all information required to successfully install the software application. Information in this document includes System Overview, Software Inventory, Hardware Requirements, Installation and Uninstall, Instructions, Configuration and User Registration Instructions, Referenced Documents, Environment and System Requirements and Configuration, and Security Requirements. Additional instructions are provided to the installer to verify the software application is installed, configured, and operating correctly. This document is required for every delivery of the software application.

System Administrator’s Manual

The System Administrator’s Manual is intended to provide all information required by the system administrator of the software application to manage the application. Information in this document includes System Overview, Referenced Documents, System Administrator Utilities, Operation and Maintenance Procedures, and Error Recovery utilities. This document references the Installation Procedures and User’s Manual for information that may be needed to conducted administrator functions. It provides detailed procedures for all maintenance and operating utilities. These include day-to-day operations, security procedures, and backup and recovery. This document is delivered for every version of the software application released.